Microsoft

Software-defined networking is built in

with Windows Server 2016

New networking approach supports innovation, helps secure workloads

Large networks are complex to configure and tricky to maintain. As data volumes grow and the pace of change accelerates, it can be a struggle to keep up. Network downtime can be caused by administrative errors with configuration, an attack that finds a new way in, or unmet user demand. What's more, the network is often blamed even when the issue lies elsewhere.

Network operators can reduce their risk profile and costs, without giving up control, by adopting a software-defined approach. Software-defined networks increase agility, mitigate emerging security threats, and provide cost-optimized performance to make IT and network administrators happier.

Software-defined networking separates network control from the data path and places it in software built to do only one thing—make sure your network is always in its desired state. This allows administrators to focus on meeting user requirements and respond faster when important issues arise. Provisioning can take place using familiar tools and be integrated with deployment processes. This lets you reduce cycle time for each request.

Many organizations are already reaping the benefits of virtualizing network traffic without needing to reengineer their base physical network infrastructure. A wide variety of network hardware is being virtualized—switches, routers, firewalls, gateways, and load balancers. These virtual networks provide isolation between workloads, tenants, and business units, and support the ability to enforce fine-grained network policy.

With Windows Server 2016, the network controller—the brains of the network—provides a central, programmable point of automation to manage, configure, monitor, and troubleshoot virtual network services in your datacenter. The network controller helps automate the configuration of network infrastructure and eliminates the need to perform manual configuration of network devices and services. With this software-based command center, network policies can be more quickly and reliably defined, realized, and monitored.

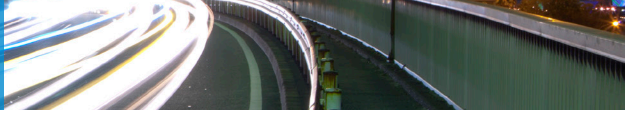
> "The ability to spin up a software-defined network in about eight minutes while eliminating a $20,000 cost is a huge benefit."
>
> – Chris Amaris
> Chief Technology Officer
> Convergent Computing

Cloud-inspired technology

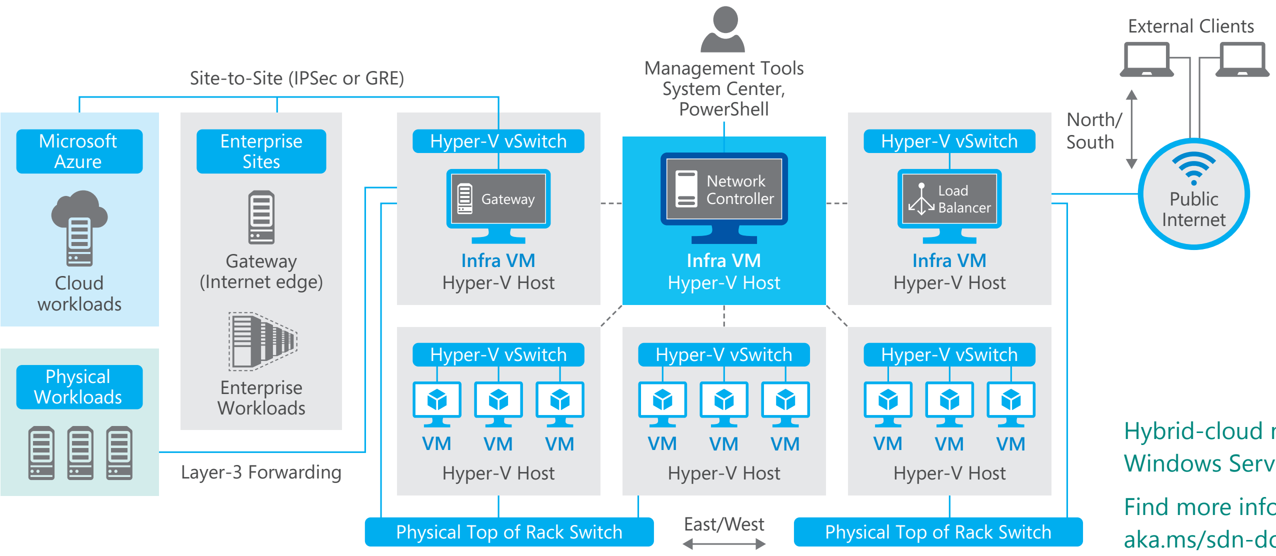
The software-defined technology built into Windows Server 2016 offers organizations access to many of the same powerful tools Microsoft uses to support Azure, its global public-cloud. Customers can put these technologies to work running their datacenters with cloud efficiencies:

- Deploy workloads and network policy quickly on top of an existing physical network.
- Micro-segment workloads for greater security using network security groups; respond quickly to new threats.
- Deliver cost-optimized performance with converged networking, scale-out software load balancing, and hybrid software-defined networking gateways.

Software-defined networking is built in



What IT wants	How Windows Server 2016 helps	Where to start
Ability to deploy applications quickly	Minimize impact on the physical network as application requirements change. Use software-defined networking (SDN) and the network controller to manage by policy, using PowerShell. Improve self service. With policy-based management and APIs, DevOps teams can deploy apps based on network and security policies.	Deploy Hyper-V and use the **network controller** to create **VXLAN overlays**. No need to re-IP the network or reconfigure physical switches. As DevOps teams deploy new workloads, the network admin retains visibility into what's happening on the network.
	Support multi-site connectivity among datacenters, physical resources, and Microsoft Azure.	Improve ability to consume resources with pooling, then use **hybrid SDN gateways** to assign and manage resources independently.
Greater security and isolation of workloads	Manage Internet traffic differently than datacenter traffic, based on security concerns and risk management tactics.	Create **network security groups** for workloads using the **distributed firewall** for microsegmentation. Establish different North-South (Internet) and East-West (intranet) traffic. Define security down to a per-VM NIC basis. Configure **User-Defined Routing** and service chains if you use third party virtual appliances, such as another firewall, load balancer, or content inspection.
Cost-optimized performance	Consolidate network infrastructure.	Replace redundant infrastructure by converging storage and network traffic on Ethernet, and activate **RDMA**.
	Extend service life so you can buy new equipment when you're ready, instead of when users complain.	Use **Switch Embedded Teaming** to combine two 10Gb ports to get 20Gb to the server, for a big network boost without additional load on the CPU.
	Improve overall throughput and helps ensure high-priority apps get the network and storage access they need.	Activate offloads for **Virtual Machine Multi-Queue** to improve throughput. Enable the built-in **software load balancer** to distribute incoming requests using policies set up through the **network controller**. Configure **Quality of Service** to prioritize traffic to critical apps.



Hybrid-cloud networking with Windows Server 2016 SDN

Find more information at aka.ms/sdn-docs.

Take the next step. Learn more at www.microsoft.com/en-us/cloud-platform/software-defined-networking

Microsoft